72% of companies restrict access to social networking

MOSCOW, RUSSIA: The 'Global IT Security Risks' survey conducted by Kaspersky Lab in partnership with B2B International, uncovered the employee activities that are most frequently subjected to restrictions. Social networks are seen as one of the greatest security threats, along with various forms of file sharing.

Access to social networking is completely blocked in 53% of companies, while another 19% restrict this kind of user activity in some way. This made social networking the second most frequently banned activity after peer-to-peer file sharing. Other frequently restricted activities include online gaming, access to certain websites, video streaming and instant messaging services.

Social networking viewed as a dangerous activity

When asked about the most dangerous employee activities, social networking was cited by 35% of businesses. "Companies are concerned about productivity as well as security, and this defines the scope of restricted employee activities," said Costin Raiu, director of Kaspersky Lab's Global Research & Analysis Team. "Social networking is seen as a time-consuming activity, but also as a potential source of malware attacks and a threat to confidential data."

Social networks have recently become one of the major channels of malware distribution, thanks to their popularity and emerging vulnerabilities in these online resources. The most notable vulnerability in Twitter, for example, led to malware infection when users simply viewed an infected message. According to Kaspersky Lab experts, social networks are being targeted by numerous attacks, so the concern shown by companies in this matter is completely justified.